UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/051,276	01/22/2002	Atsushi Shimbo	04329.2725	7600

			EXAMINER
22852	7590	01/31/2006	PATEL, NIRAV B

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER
LLP
901 NEW YORK AVENUE, NW
WASHINGTON, DC 20001-4413

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 01/31/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

	Application No.	Applicant(s)
Office Action Summary	10/051,276	SHIMBO ET AL.
	Examiner	Art Unit	
	Nirav Patel	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _December 12, 2005 (Amendment)_.

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-16_ is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-16_ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____.

DETAILED ACTION

1. This action is in response to the amendment dated on December 12, 2005.

2. Claims 1-16 are under pending.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Iwamura et al. (US Patent No. 5,321,752) and further in view of Sathi Perumal ("Pipelined 50 MHz CMOS ASIC for 32 bit Binary to residue conversion and residue to binary conversion" 1994).

As per claim 1, Iwamura teaches:

A *modular exponentiation calculation apparatus* [*col. 6 lines 5-9* "a communication apparatus which performs encryption or decryption of a communication content by using a modular exponentiation $C=M^e$ mod N concerning integers M and e using N as the modulus, the communication apparatus comprising"] which utilizes a *residue number system* [*col. 3 lines 50-53* "modular exponentiation and modular multiplication employed in cryptic communication is executed simply by repeating modular multiplication using R which is prime to N which is the

residue"] representation by a first base and a second base including sets of a plurality

of integers with respect to object data C and parameters p, q, d (all integers included in

both the bases are mutually primary, a product "A" of all the integers of the first base is

A>p, A>q, a product "B" of all the integers of the second base is B>p, B>q, and A X

B>C) to obtain a calculation result m=C^d mod (p X q) **[*col. 4 lines 40-41* "the modular**

exponentiation C=M^e mod N is executed", *col. 1 lines 13-24* "computation known

as modular exponentiation which is expressed by C=M^e mod N(C,M,N,e), where E,

M, N and e are integers"], said apparatus comprising:

a first processing unit configured to obtain a residue number system representation of a

value Cp^{dp} *X B mod p* or a value with p *added* thereto based on a residue number

system representation of a remainder value Cp=C mod p by p of said data C and a

remainder value dp=d mod (p-1) by (p-1) of said parameter d **[*col. 1 lines 14-24***

"encryption of data to transmit and decryption of received cryptogram by using a

computation in which two integers A and B are multiplied with each other and the

product is divided by a third integer N to determine the residue, i.e., modular

multiplication expressed by A•B mod N", *col. 3 lines 63-68*, *col. 4 lines 1-3*

"executing a modular multiplication A•B mod N of integers A and B by using N as

the modulus, the communication apparatus having at least one computing unit

which computes and outputs Z=U•V•R^{-1} mod N by using an integer R which is

primer to N, the method comprising the steps of: inputting to one of the

computing units A and a constant R$_R$ which is expressed by R$_R$ =R$_2$ mod N,

thereby causing the computing unit to output A$_R$ =A•R$_R$• R^{-1} mod N" *col. 9 lines*

65-68, col. 10 lines 1-2 "addition of E_{j-1} as the residue are conducted. That is, L_{j-1} is converted into E_{j-1} and the thus obtained E $_{j-1}$ is added. By this method, all the subtractions made by mod N can be carried out by adding computations"];

a second processing unit configured to obtain a residue number system representation of a value Cp^{dp} X B mod q or a value with q added thereto based on a residue number system representation of a remainder value Cq=C mod q by q of said data C and a remainder value dq=d mod (p-1) by (q-1) of said parameter d **[col. 4 lines 3-5 inputting to one of the computing units B and the constant R_R thereby causing the computing unit to output B_R =B•R_R•R^{-1} mod N]**;

a third processing unit configured to obtain a residue number system representation of an integer m' congruent with $m=C^d$ mod (p X q) **[col. 4 line 23 "constant R_R which is expressed by $R_R=R^2$ mod N"]**, based on both the residue number system representations obtained by said first and second processing units **[col. 4 lines 6-8 "inputting to the computing unit the A_R and B_R thereby causing the computing unit to output T_R =A_R•B_R•R^{-1} mod N"]**; and

Iwamura teaches the apparatus comprising four various processing unit (i.e. four various computing means *col. 6 lines 19-32*). Iwamura doesn't expressively mention that calculate result by *converting RNS (residue number system) to binary* representation.

However, Sathi Perumal teaches the Residue to Binary conversion **[page 456 lines 23-25 "if two residue number Z1 and Z2 are known, then the binary number equivalent B can be calculated from (13)"]**.

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate the teaching Sathi Perumal into the teaching of Iwamura to use RNS to Binary converter. The modification would be obvious because one of ordinary skill in the art would be motivated to use residue to binary converter (RBC) to convert the 8 RNS moduli words to a unique 32 bit binary number. The result is a complete simulated pipelined design which supports a clock frequency of 50 MHz **[Sathi Perumal, *page 454 lines 5-10*]**.

As per claim 2, the rejection of claim 1 is incorporated and further Iwamura teaches:

first processing unit performs a residue number system *Montgomery multiplication* of the residue number system representation of said remainder value Cp and the residue number system representation of B^2 mod p **[*col. 27 lines 23-50* "in executing Montgomery modular multiplication, R is an integer prime to N on condition that R is determined to be 2^n (n being an optional integer). In this case, the division by R can simply be performed by a bit-shift operation, so that the Montgomery modular multiplication of the formula (25) or (27) is executed simply by multiplication alone"]**, performs a residue number system *Montgomery exponentiation* using said remainder value dp as an exponent portion with respect to the obtained residue number system representation, and thereby obtains the residue number system representation of the value Cp^{dp} X B mod p or the value with p added thereto **[*col. 27 lines 52-66, col. 28 lines 1-9* "it is thus possible to carry out modular**

exponentiation only by Montgomery modular multiplication. The initial value of C_R in formula (30) can be treated as a constant which is determined by R_R and N. The described modular exponentiation conducted through Montgomery modular multiplication alone will be referred to a Montgomery modular exponentiation", *col. 29 lines 47-50, col. 30 lines 1-2*], and

second processing unit performs a residue number system *Montgomery multiplication* of the residue number system representation of said remainder value Cq and the residue number system representation of B^2 mod q [*col. 27 lines 23-50* "in executing **Montgomery modular multiplication, R is an integer prime to N on condition that R is determined to be 2^n (n being an optional integer). In this case, the division by R can simply be performed by a bit-shift operation, so that the Montgomery modular multiplication of the formula (25) or (27) is executed simply by multiplication alone"**], performs a *residue number system Montgomery exponentiation* using said remainder value dq as the exponent portion with respect to the obtained residue number system representation, and thereby obtains the residue number system representation of the value Cp^{dq} X B mod q or the value with q added thereto [*col. 27 lines 52-66, col. 28 lines 1-9* "**it is thus possible to carry out modular exponentiation only by Montgomery modular multiplication. The initial value of C_R in formula (30) can be treated as a constant which is determined by R_R and N. The described modular exponentiation conducted through Montgomery modular multiplication alone will be referred to a Montgomery modular exponentiation**" *col. 29 lines 47-50, col. 30 lines 1-2*].

As per claim 3, the rejection of claim 2 is incorporated and further Iwamura teaches:

a unit configured to obtain said *remainder value* (i.e. residue calculation) dp and said remainder value dq based on said parameters p, q, and d [*col. 20 lines 20-30* **"$S_{j-1,n-1}$•**

$X^n + E_{j-1}$ is executed in place of executing Q_{j-1} *N, so that the residue calculation is performed. $S_{j-1, n-1}$ * X^n is automatically performed due to the overflow of $S_{j-1, n-1}$, the residue calculation can be completed only by adding E_{j-1}"].

As per claim 4, the rejection of claim 1 is incorporated and further Iwamura teaches:

third processing unit performs a residue number system *Montgomery multiplication* of said residue number system representation obtained by said first processing unit and the residue number system representation of an inverse element qinv=q^{-1} mod p in a modulus p of said parameter q [*col. 27 lines 16-18* **"The Montgomery modular multiplication can be expressed as follows:**

T_R =A_R•B_R•R^{-1} mod N=(A_R•B_R + M•N)/R"], performs a *residue number system multiplication* (i.e. residue multiplication) of the obtained residue number system representation [*col. 18 lines 48-54* **"the calculation of the RSA cryptography to be performed on the basis of the Chinese Reminder Theorem can basically be executed in parallel. Therefore, it is most suitable for use in the method according to the present invention in which the residue multiplication is executed by a plurality of calculating apparatus"**] and the residue number system

representation of said parameter q, performs a residue number system *Montgomery multiplication of said residue number system* representation obtained by said second processing unit and the residue number system representation of an inverse element pinv=p^{-1} mod q in a modulus q of said parameter p [*col. 27 lines 16-18* "**The Montgomery modular multiplication can be expressed as follows:**

T_R =A_R•B_R•R^{-1} mod N=(A_R•B_R + M•N)/R"], performs a *residue number system multiplication* of the obtained residue number system representation and the residue number system representation of said parameter p [*col. 18 lines 48-54* "**the calculation of the RSA cryptography to be performed on the basis of the Chinese Reminder Theorem can basically be executed in parallel. Therefore, it is most suitable for use in the method according to the present invention in which the residue multiplication is executed by a plurality of calculating apparatus**"], performs a residue number system *addition* of both obtained results of a residue number system multiplication [*col. 12 lines 14-16* "**FIG. 3 illustrates a circuit for executing basic calculation R=R*X + A_{n-j} *B mod N of the residue multiplication and called a basic operator**" (i.e. addition of residue multiplication)], and obtains the residue number system representation of the integer m' as the combination with C^d in said modulus p X q (i.e. modular exponentiation) [*col. 27 lines 52-68* "**Modular exponentiation C=M^e mode N also can be conducted as follows by using Montgomery method**" *col. 28 lines 1-4* "**it is thus possible to carry our modular exponentiation only by Montgomery modular multiplication**"].

As per claim 5, the rejection of claim 4 is incorporated. Iwamura doesn't

teach that convert the *binary representations to the RNS* (Residue number system).

However, Sathi Perumal teaches the Binary to residue conversion [*page*

454, 455 **equation (5) Fig. 2]**.

Therefore, it would have been obvious to a person of ordinary skill in the

art at the time the invention was made to incorporate the teaching of Sathi Perumal into

the teaching of Iwamura to use Binary to residue converter. The modification would be

obvious because one of ordinary skill in the art would be motivated to use BRC (Binary

to residue Conversion) which employs a unique inverted tree structure that permits very

fast clock frequencies while at the same time maintaining an area-efficient design **[Sathi**

Perumal *page 454 lines 35-37]*.

As per claim 6, the rejection of claim 5 is incorporated and further

Iwamura teaches:

unit configured to obtain the *inverse element* pinv and the inverse element qinv in the

modulus p of said parameter q based on said parameters p and q [*col.* **5** *lines 14-16*

"computing $A_R \cdot B_R \cdot R^{-1}$ mod N on the basis of the computing results A_R and B_R and

the R, thus determining T_R as the computation result; and computing $T_R \cdot R^{-1}$ mod

N on the basis of the T_R and the R"].

As per claim 7, the rejection of claim 1 is incorporated and is rejected for

the same reason set forth in the rejection of claim 3 above.

As per claim 8, the rejection of claim 1 is incorporated and further Iwamura teaches:

a *storage unit* configured to store data of a residue number system representation depending only on said parameters p, q, d [*col. 6 lines 59-60* "**fourth computing means which computing , upon receipt of C$_r$ stored in the first storage means**"].

As per claim 9, the rejection of claim 1 is incorporated and is rejected for the same reason set forth in the rejection of claim 8 above.

As per claim 10, the rejection of claim 1 is incorporated and further Iwamura teaches:

first processing unit and said second processing unit execute at least a part of a processing at the *same time* (i.e. parallel processing or pipeline processing) [**Fig. 4** *col. 12 lines 22-25* "**The systolic array performs the calculation by a pipeline processing by PEs which are small and same functional blocks**"].

As per claim 11, the rejection of claim 1 is incorporated and is rejected for the same reason set forth in the rejection of claim 10 above.

As per claim 12, the rejection of claim 1 is incorporated and further Iwamura teaches:

a unit configured to set a value of said integer m' less than p X q obtained by the subunit or a value less than p X q obtained by *subtracting* a predetermined number p X q from said integer m' not less than p X q to m=C^d mod p X q [*col. 9 lines 65-68, col. 10 lines 1-2 "instead of execution of $-Q_{j-1} \cdot N$ which is $L_{j-1} \cdot X^n$ mod N, subtraction of $L_{j-1} \cdot X^n$ and addition of E_{j-1} as the residue are conducted. That is, L_{j-1} is converted into E_{j-1} and the thus obtained E_{j-1} is added. By this method, all the subtractions made by mod N can be carried out by adding computations"*].

As per claim 13, the rejection of claim 1 is incorporated and further Iwamura teaches:

the number of elements of said first base is the *same as* the number of elements of said second base [*col. 10 lines 57-59 "the modular exponentiation can be realized by repeating the modular multiplication C = C·B mod N (B is M or C)"*].

As per claim 14, it is a method claim corresponds to apparatus claim 1 and is rejected for the same reason set forth in the rejection of claim 1 above.

As per claim 15, it is a computer usable medium claim corresponds to apparatus claim 1 and is rejected for the same reason set forth in the rejection of claim 1 above. Further Iwamura teaches that computer usable medium [*col. 8 line 31*].

As per claim 16, it is an apparatus claim corresponds to apparatus claim 1

and is rejected for the same reason set forth in the rejection of claim 1 above.

Response to Argument

4. Applicant's arguments filed December 12, 2005 have been fully considered but

they are not persuasive.

Applicant argues that:

"Iwamura does not utilize residue number system representations". Iwamura

does not teach a modular exponentiation calculation apparatus utilizing residue number

system representations".

Examiner maintains that:

Iwamura teaches the circuit to perform high-speed modular multiplication or

modular exponentiation. The repetition of computation is executed by repeatedly

operating a single circuit or by simultaneously operating a plurality of circuits of the

same construction in a parallel manner **[abstract]**. Iwamura teaches the modular

exponentiation $C = M^e$ mod N concerning integers M and e using N as the modulus **[col.

4 lines 15-17]** and communication unit which computes and outputs $Z = U.V.R^{-1}$ mod

N by using, which respect to input data U and V, an integer R which is primer to N **[col.

4 lines 18-21]**. Iwamura teaches the residue number system representations (i.e. binary

expression of e) **[col. 4 lines 25-27, "the computing unit to output $M_R = M.R_R.R^{-1}$**

mod N; representing the binary expression of e by e = [e^t, e^{t-1}, ..., e^1]" (i.e. which is expressed as a set)] and modular exponentiation calculation using the residue number system representations [col. 4 lines 28-41 "after completion of processing on all e^i, inputting the C_R and 1 as a constant to one of the computing units, thereby causing the computing unit to output, as the aimed C, C = C_R.1.R^{-1} mod N, whereby the modular exponentiation C = M^e mod N is executed"]. Iwamura teaches the modular multiplication C = M^e mod N by repeating modular multiplication of two number [algorithm, col. 8 lines 57-68, col. 9 lines 1-6]. Iwamura teaches that computation of A.B mod N = R, where A, B and N are integers and each of A, B and N are divided by n into n sections each being of m bits (i.e. result of division into n sections, where each section contains a contributing factor as an element within number system representations set) [col. 9 lines 17-31]. Iwamura teaches the residue multiplication [Fig. 3 col. 12 lines 14-17, col. 11 lines 32-38, col. 22 lines 51-64] and the systolic array (which performs the calculation by a pipeline processing) [Fig. 4]. Iwamura teaches the residue calculation that can be completed by adding E_{j-1} [col. 20 lines 20-40 "E_{j-1,n-1} (i=1, ..., n) are sequentially transmitted at timing signal T_{m-1} synchronized with B_{n-i}" (i.e. more than one element such as a set is required for calculation)]. Iwamura teaches the Moldular Multiplication using the Montgomery method [col. 26 lines 37-55, col. 27 1-24, lines 52-60] as claimed.

Applicant argues that:

"Perumal does not cure deficiencies of Iwamura and therefor there is no motivation to combine the teachings in Iwamura with the teaching in Perumal".

Examiner maintains that:

Iwamura teaches the circuit to perform high-speed modular multiplication or modular exponentiation. Iwamura teaches the residue number system representations (i.e. binary expression of e) **[col. 4 lines 25-27, "the computing unit to output M_R = $M.R_R.R^{-1}$ mod N; representing the binary expression of e by e = $[e^t, e^{t-1}, ..., e^1]$ (i.e. which is expressed as a set)"]** and modular exponentiation calculation using the residue number system representations **[col. 4 lines 28-41 "after completion of processing on all e^i, inputting the C_R and 1 as a constant to one of the computing units, thereby causing the computing unit to output, as the aimed C, C = $C_R.1.R^{-1}$ mod N, whereby the modular exponentiation C = M^e mod N is executed"]**. Perumal discloses the Residue number system (RNS) processor architecture Binary to Residue conversion (BRC) and Residue to Binary conversion (RBC) **[page 454, 455 (i.e. two-way conversation)]**. The modification would be obvious because one of ordinary skill in the art would be motivated to use residue to binary converter (RBC) to convert the 8 RNS moduli words to a unique 32 bit binary number. The result is a complete simulated pipelined design, which supports a clock frequency of 50 MHz **[Sathi Perumal, *page 454 lines 5-10*]**. Furthermore, the examiner recognizes that obviousness can only be established by combining or modifying the teaching of the prior art to produce the

i

claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to on of ordinary skill in the art. See *In re Fine*, 837 F. 2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and In re Jones, 958 F.2d 347, 21 USPQ 2nd 1941 (Fed. Cir 1992). In this case, the combination of Iwamura and Perumal teach the claimed subject matter and the combination is sufficient.

Conclusion

5. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

Robert Hohne ("A Programmable High Performance processor using the Residue Number System and CMOS VLSI technology", 1989 IEEE, page 41-43).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nirav Patel whose telephone number is 571-272-5936. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax and phone numbers for the organization where this application or proceeding is assigned is 571-273-8300.

Any inquiry of a general nature or relating to the status of this application or

proceeding should be directed to the receptionist whose telephone number is 571-272-

2100.

NBP

1/26/06

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100